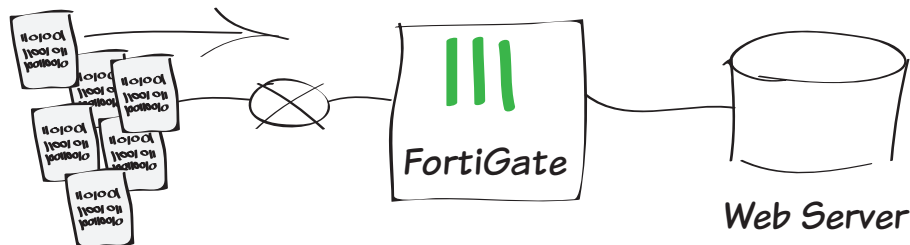


# Protecting a web server from common external attacks

In this example, you will protect a web server using an Intrusion Prevention System (IPS) profile and a Denial of Service (DoS) policy. This will prevent a variety of different attacks from reaching the server.

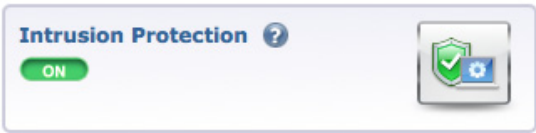
1. Enabling Intrusion Protection
2. Configuring the default IPS profile to block common attacks
3. Adding the IPS sensor to the server access security policy
4. Creating a DoS policy
5. Results

External Attacks



1. Enabling Intrusion Protection

Go to **System > Config > Features** and ensure that **Intrusion Protection** is turned **ON**. Apply your changes if necessary.



2. Configuring the default IPS profile to block common attacks

Go to **Security Profiles > Intrusion Protection** and edit the **default** profile. In the **Pattern Based Signatures and Filters** list, highlight the default entry and select **Edit**.

Pattern Based Signatures and Filters				
Create New	Edit	Delete		
Severity	Target	OS	Action	Matched Signatures
Medium, High, Critical	All	All	Default	3Com.3CDaemon.FTP.Server.Buffer.Overflow 3Com.Intelligent.Management.Center.Directory.Traversal ... [Show all 4577]

Select **Severity** to view all signatures in the database.

Severity	Target	OS
<input checked="" type="checkbox"/> Critical	<input checked="" type="checkbox"/> client	<input checked="" type="checkbox"/> BSD
<input checked="" type="checkbox"/> High	<input checked="" type="checkbox"/> server	<input checked="" type="checkbox"/> Linux
<input checked="" type="checkbox"/> Medium		<input checked="" type="checkbox"/> MacOS
<input checked="" type="checkbox"/> Low		<input checked="" type="checkbox"/> Other
<input checked="" type="checkbox"/> Information		<input checked="" type="checkbox"/> Solaris
		<input checked="" type="checkbox"/> Windows

Scroll down and set the **Action** to **Block All**.

Action	<input checked="" type="checkbox"/> Signature Defaults	<input checked="" type="checkbox"/> Monitor All	<input checked="" type="checkbox"/> Block All	<input checked="" type="checkbox"/> Reset	<input checked="" type="checkbox"/> Quarantine
--------	--	---	---	---	--

Enable all the listed **Rate Based Signatures**.

Rate Based Signatures						
Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
	Apache.HTTP.Server.Range.DoS	30	1	Any	Block	0
	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	Block	0
	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	Block	0
	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block	0
	FTP.Login.Brute.Force	200	10	Any	Block	0
	FreeBSD.TCP.Reassembly.DoS	10	2	Any	Block	0
	IMAP.Login.Brute.Force	60	10	Any	Block	0
	Lotus.Domino.Login.Brute.Force	300	10	Any	Block	0
	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Any	Block	0
	MS.RDP.Connection.Brute.Force	200	10	Any	Block	0
	MS.Windows.SMB.NTLM.Authentication.Lack.Of.Entropy	35	1	Any	Block	0
	MS.Windows.SMB.Server.NTLM.Authentication.Bypass	1000	1	Any	Block	0
	MS.XML.Core.Services.Memory.Corruption	5	10	Any	Block	0
	MySQL.Login.Brute.Force	60	60	Any	Block	0
	Novell.Open.Enterprise.Server.HTTPSTK.DoS	19	1	Any	Block	0
	POP3.Login.Brute.Force	200	10	Any	Block	0
	SMB.Login.Brute.Force	500	60	Any	Block	0
	SSH.Connection.Brute.Force	200	10	Any	Block	0
	Telnet.Login.Brute.Force	60	60	Any	Block	0
	Wordpress.Login.Brute.Force	1000	10	Any	Block	0

3. Adding the *IPS sensor* to the *server access security policy*

Go to **Policy & Objects > Policy > IPv4** and edit the security policy allowing traffic to the web server from the Internet.

Enable **IPS** under **Security Profiles** and set it to use the **default** profile.

Enabling IPS automatically enables **SSL Inspection**. Set this feature to use the **certificate-inspection** profile.

Incoming Interface	wan1	
Source Address	all	
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	internal	
Destination Address	all	
Schedule	always	
Service	ALL	
Action	ACCEPT	
<b>Firewall / Network Options</b>		
NAT		
Use Destination Interface Address		Fixed Port
Use Dynamic IP Pool		Click to add...
<b>Security Profiles</b>		
AntiVirus		default
Web Filter		default
Application Control		default
IPS		default
SSL Inspection		certificate-inspection

4. Creating a DoS policy

Go to **Policy & Objects > Policy > DoS** and create a new policy.

Set **Incoming Interface** to your Internet-facing interface.

In the **Anomalies** list, enable **Status** and **Logging** and set the **Action** to **Block** for all types.

Incoming Interface

wan1

Source Address

all

Destination Address

all

Service

ALL

Anomalies

Name	<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Logging	Action	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
tcp_port_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	1000
tcp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
tcp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
udp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
udp_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
udp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
udp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
icmp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	250
icmp_sweep	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	100
icmp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	300
ip_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
sctp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
sctp_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	1000
sctp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
sctp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000

ON

Enable this policy

5. Results



DoS attacks are illegal, unless you own the server under attack. Before performing an attack, ensure that you have the correct server IP.

Launch a DoS attack on your web server’s IP address.

Go to **System > FortiView > Threats** and select the **5 Minutes** view.

You will see that a DoS attack has been detected and blocked.

